Inheritatie in multidomein-omgeving in FTD

Inhoud

Inleiding

Dit document beschrijft de configuratie en het werken van erfopvolging en multi-domein eigenschappen. Dit richt zich ook op een real-world use case om te zien hoe deze twee eigenschappen samen werken.

Voorwaarden

Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- FireSIGHT Management Center (FMC)
- Firepower Threat Defense (FTD)

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Firepower Management Center (FMC) softwareversie 6.4
- Firepower Threat Defense (FTD) softwareversie 6.4

  Opmerking: De ondersteuning van meerdere domein- en inneringsfuncties is vanaf versie 6.0 beschikbaar bij FMC/FTD.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg ervoor dat u de potentiële impact van om het even welke configuratie begrijpt.

Achtergrondinformatie

Bij beleidscoherentie kan het toegangscontrolebeleid worden ontwikkeld waarbij het kinderbeleid regels van een basisbeleid erft, inclusief de ACS-instellingen zoals veiligheidsintelligentie, HTTP-respons, vastlegging van instellingen enz. Optioneel kan de beheerder het kinderbeleid toestaan om de ACS-instellingen te omzeilen zoals veiligheidsintelligentie, HTTP-respons, vastlegging of anders de instellingen te vergrendelen zodat het kinderbeleid ze niet kan omzeilen. Deze optie is zeer nuttig in een multi-domein FMC omgeving.

De toegang van de gebruiker tot de door het FMC beheerde apparaten, configuraties en gebeurtenissen op meerdere gebieden. Een gebruiker kan naar andere domeinen overschakelen of toegang krijgen, afhankelijk van de rechten. Als de optie voor meerdere domeinen niet is ingesteld, behoren alle beheerde apparaten, configuraties en gebeurtenissen tot het **mondiale** domein.

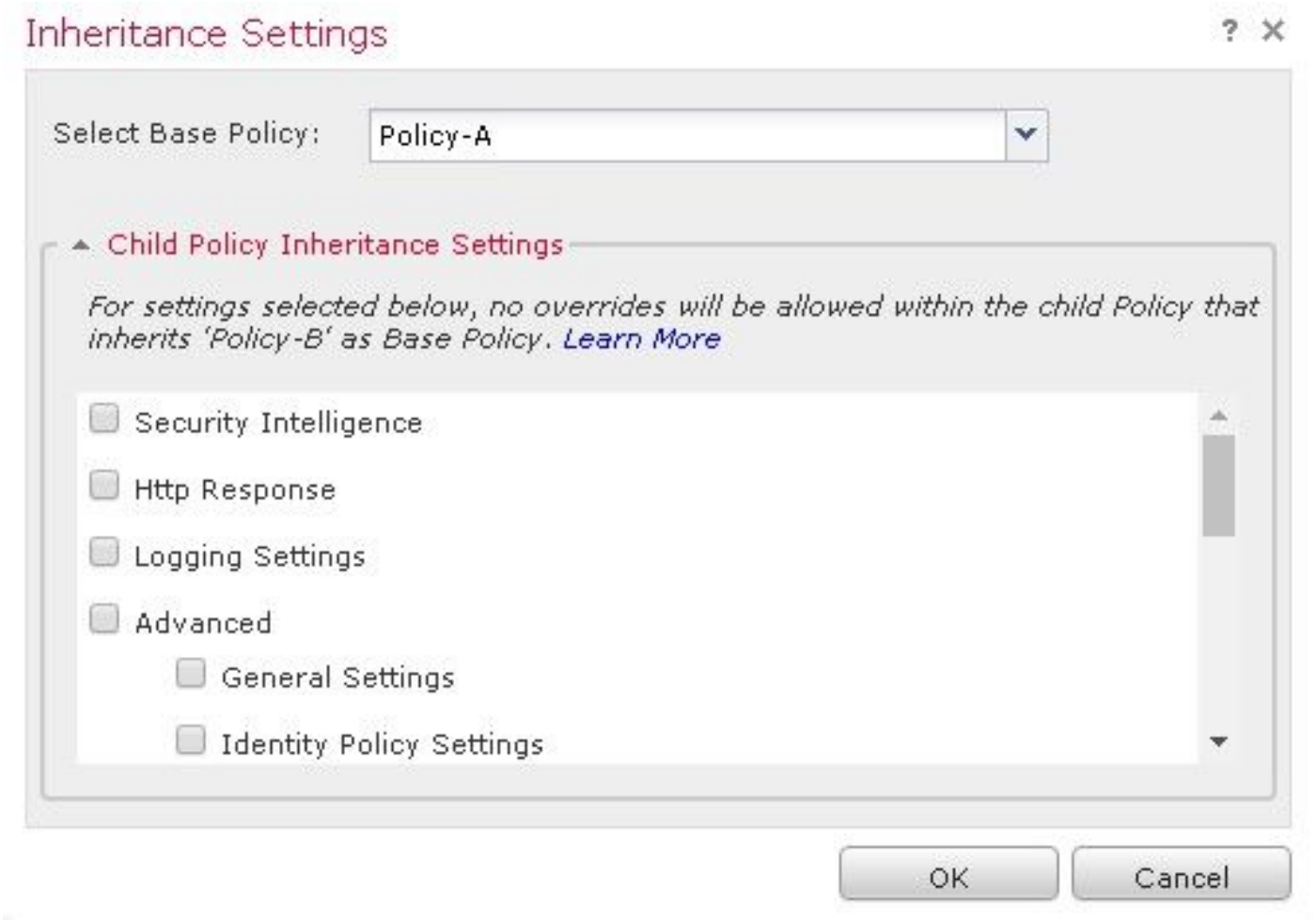
Beleidsherkenning instellen

Een bladdomein is een domein dat geen verdere subdomeinen heeft. Een kinderdomein is het volgende-niveau afstamming van het domein waar de gebruiker/admin momenteel is. Het parent-domein is de directe voorouder van het domein waar de gebruiker/admin momenteel is.

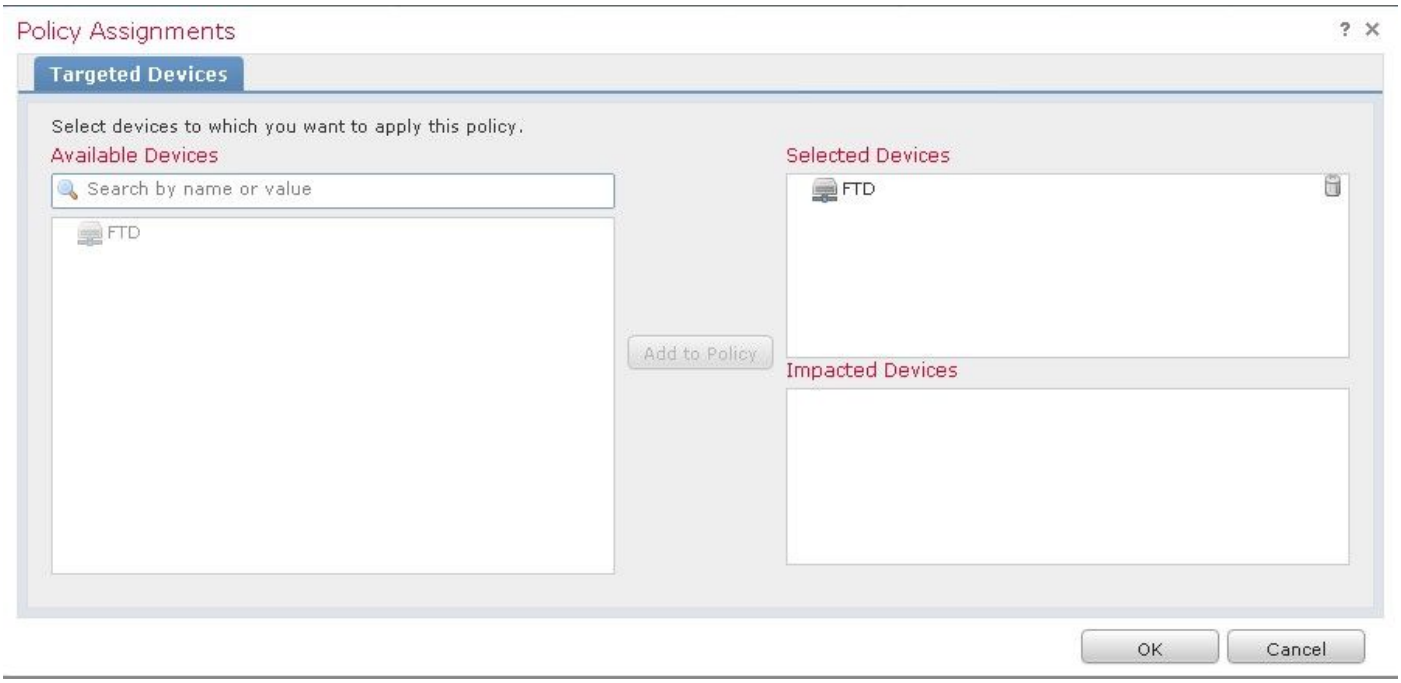
U kunt erfenis als volgt configureren/instellen voor beleid dat bestaat:

1. Let op Policy-A het basisbeleid en Policy-B het kinderbeleid (Policy-B erft de regel uit Policy-A)
2. Klik op Policy-B en op **Overeenstemmingsinstellingen** zoals in de afbeelding.

3. Selecteer Policy-A in de vervolgkeuzelijst **Base Policy** hieronder. Andere ACS-instellingen zoals veiligheidsintelligentie, HTTP-respons, vastlegging instellingen enz. kunnen worden geërfd om instellingen voor kinderbeleid te omzeilen.

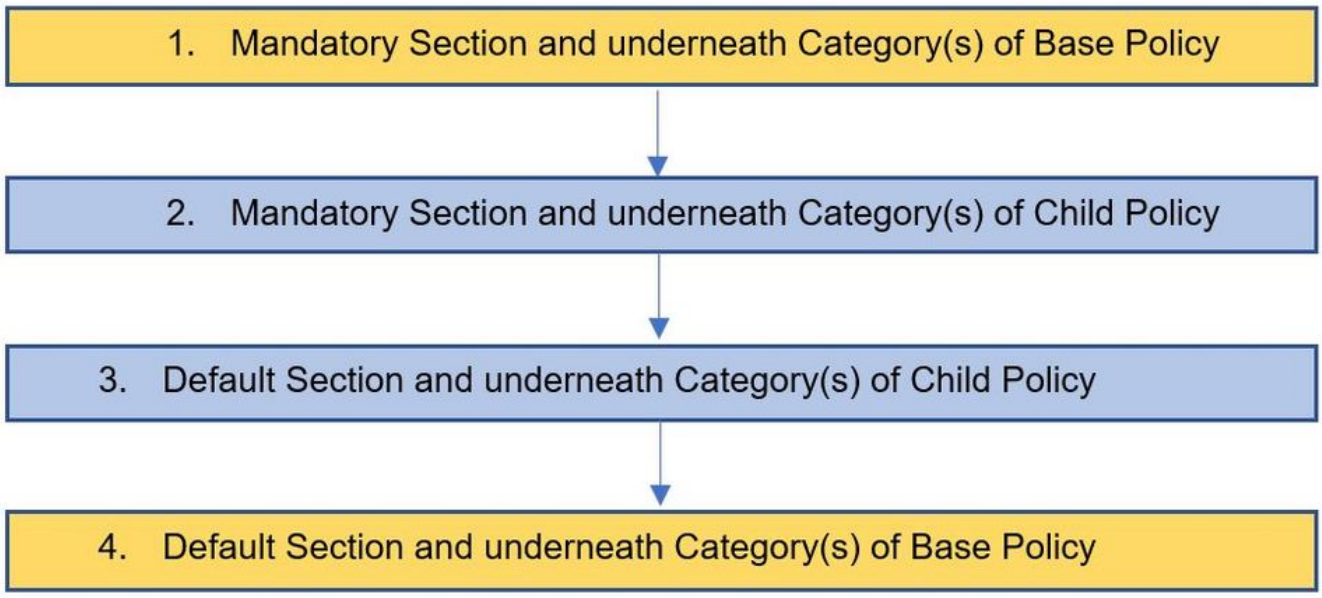


4. Doet de **beleidstoewijzing** voor het kinderbeleid-B tegen de beoogde FTD-apparatuur:

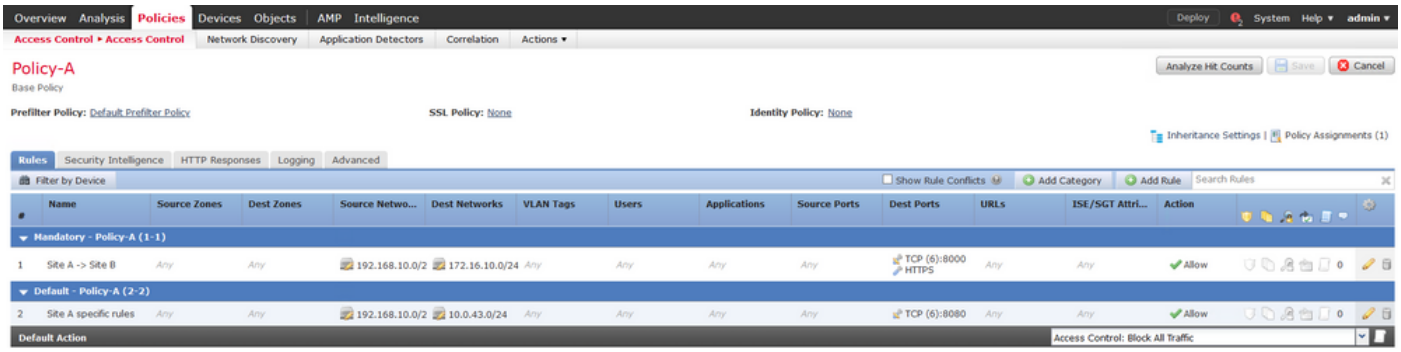


Standaard wordt de **Standaardactie** van het kinderbeleid geërfd en ingesteld op **Inherit uit basisbeleid** zoals in de afbeelding. De gebruiker heeft ook de optie om de **Standaardactie** te selecteren uit het hier weergegeven systeembeleid.

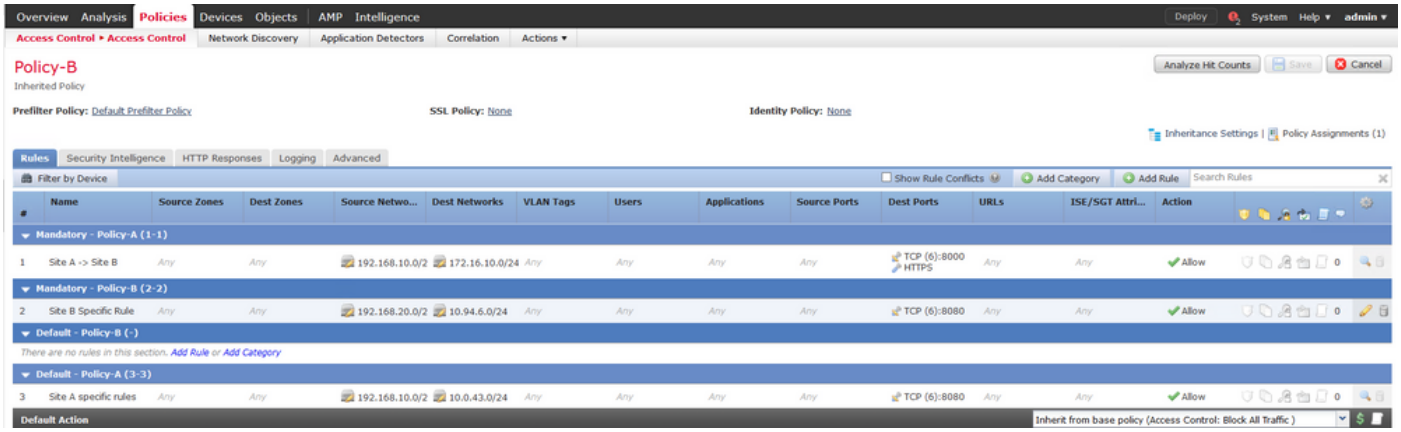
De volgorde van de opvraging voor het verkeer zal altijd van bovenaf zijn, ongeacht het aantal categorieën die in zowel de verplichte als de standaardafdelingen zijn toegevoegd. Nadat u de **Overerfeningsinstellingen** hebt toegepast**,** de ACS-vertegenwoordiging voor kinderbeleid-B (kinderbeleid) zoals weergegeven in de afbeelding, in overeenstemming met de **orde van de** eerder genoemde **regelcontrole**:



Dit beeld laat zien hoe zowel het beleid, namelijk Policy-A, dat het basisbeleid is, als het beleid-B, dat het kinderbeleid is en dat van beleid A is geërfd, in het VCC zou worden getoond.



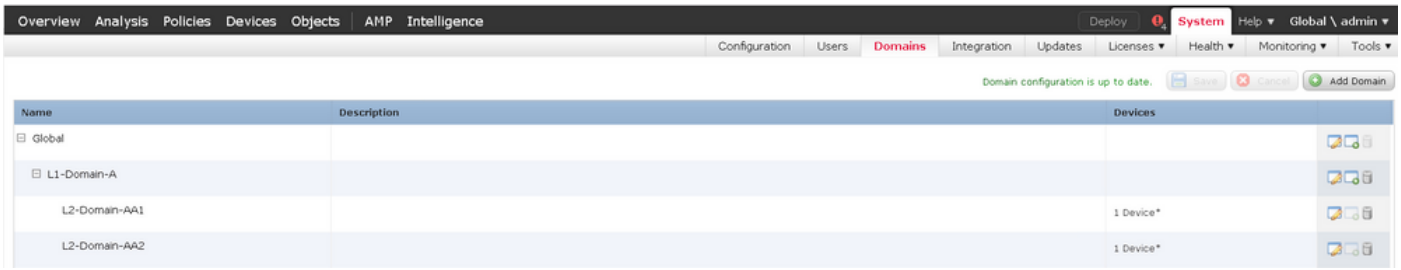
Deze afbeelding laat zien dat in Policy-B de regels uit Policy-A kunnen worden gezien evenals specifieke regels die zijn geconfigureerd in Policy-B zelf. Er moet op worden gelet hoe de regels moeten worden ingesteld, waarbij de volgorde in acht moet worden genomen.



FTD-beheer in FMC-omgeving met meerdere domeinen

De gebruikerstoegang voor meerdere domeinen is beperkt tot beheerde apparaten, configuraties en gebeurtenissen. Een gebruiker zou naar andere domeinen kunnen overschakelen, afhankelijk van de privileges. Als de optie meerdere domeinen niet is geconfigureerd, behoren alle beheerde apparaten, configuraties en gebeurtenissen tot het **mondiale** domein.

Een maximum van drie niveaus kan met Global Domain als niveau 1 worden geconfigureerd. Alle beheerde apparaten moeten alleen tot het bladdomein behoren. Dit kan worden bevestigd aan de hand van het symbool van het  (Subdomein toevoegen) dat in het bladdomein zoals in de afbeelding wordt weergegeven wordt grijswaarden weergegeven.



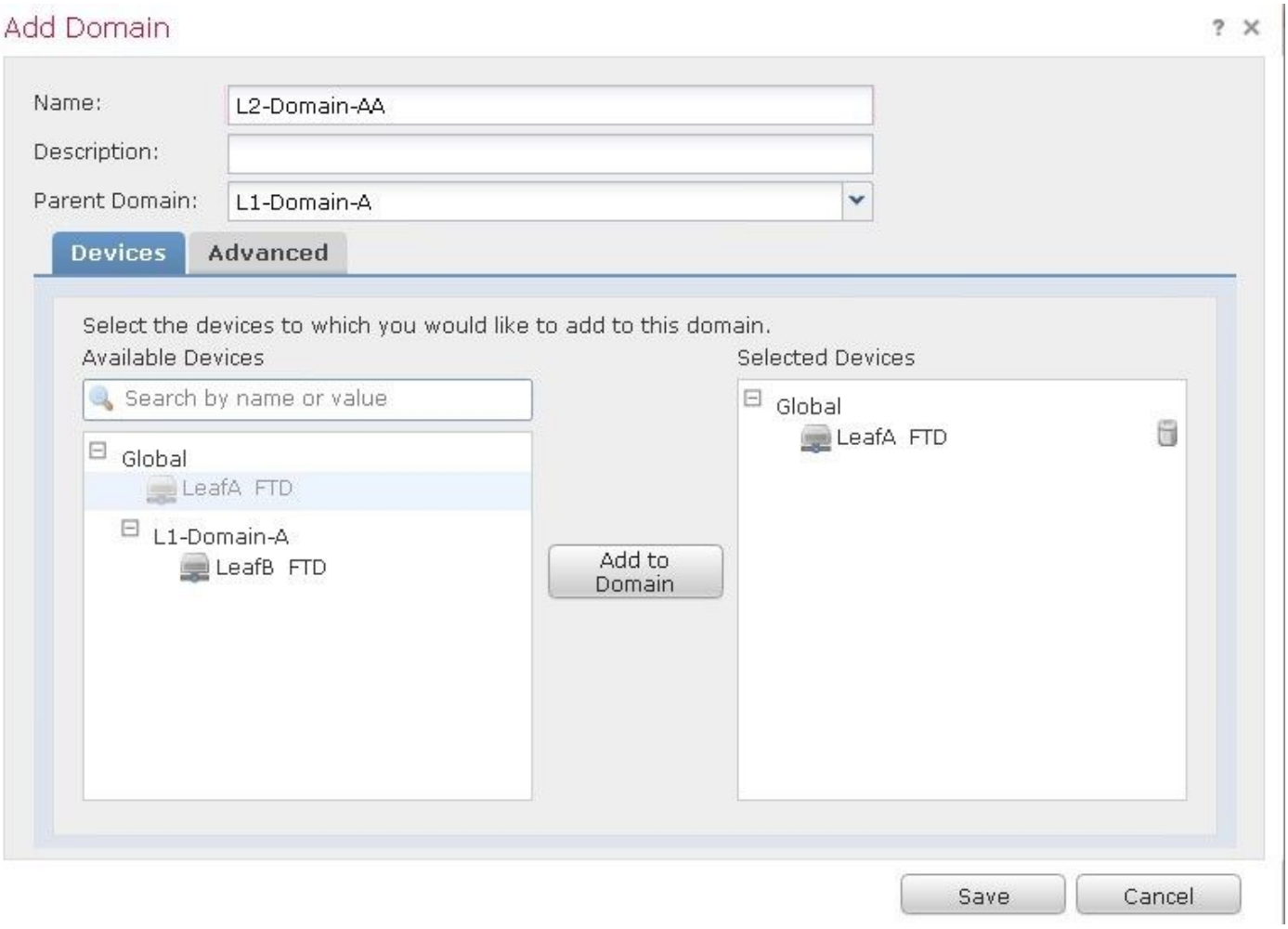
Domain Configuration

De domeinconfiguratie kan als volgt worden uitgevoerd:

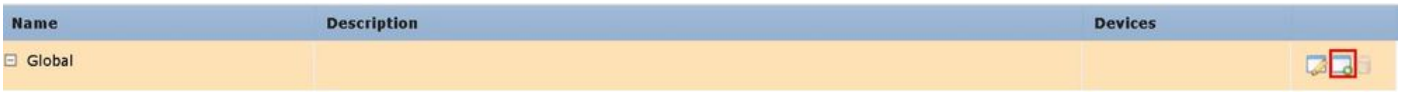
1. Blader naar **systeem > domeinen**. Standaard is het **Global**-domein aanwezig.

2. Klik op **Add Domain** zoals in de afbeelding wordt getoond.

3. Het dialoogvenster **Domain** toevoegen verschijnt. Typ de **naam** van het domein en selecteer het **Parent Domain** van een vervolgkeuzelijst. Als dit het bladdomein is, moeten de FTD-apparaten aan het domein worden toegevoegd zoals in de afbeelding.

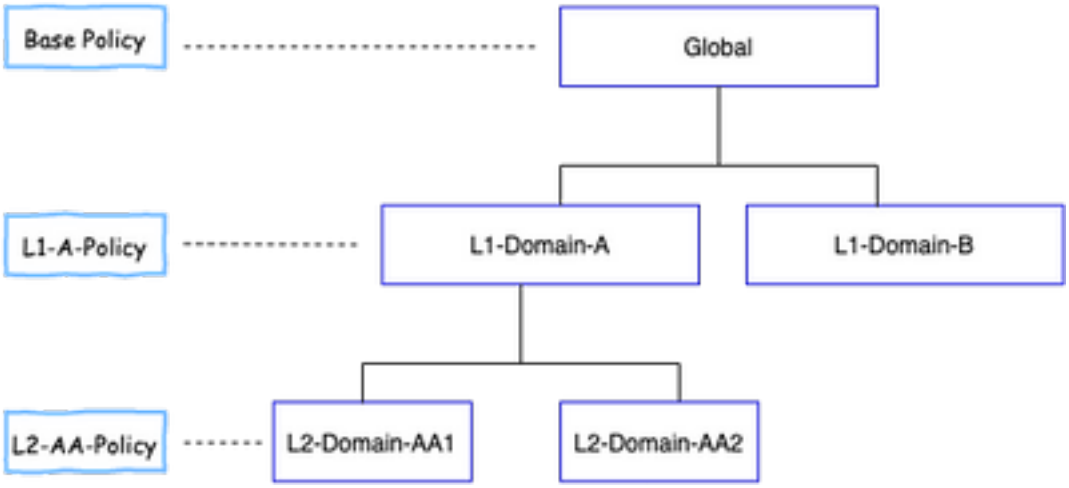


Opmerking: Om de domeinen toe te voegen, klik op het pictogram **Subdomein toevoegen** zoals in de afbeelding. Hier is het parent-domein al geselecteerd.



Policy Visibility and Control in een FMC-omgeving met meerdere domeinen

Beleidszichtbaarheid en -controle zijn beperkt tot respectieve domeingebruikers, met uitzondering van een Admin of **Global** Domain. Dit voorbeeld is als volgt gebaseerd op de hiërarchie:



Zichtbaarheid: Zoals in deze afbeelding wordt getoond, bevat de standaard-weergavebeleid, een lijst van beleidsmaatregelen (ACS) **die** onder het betreffende domein zijn ingesteld.

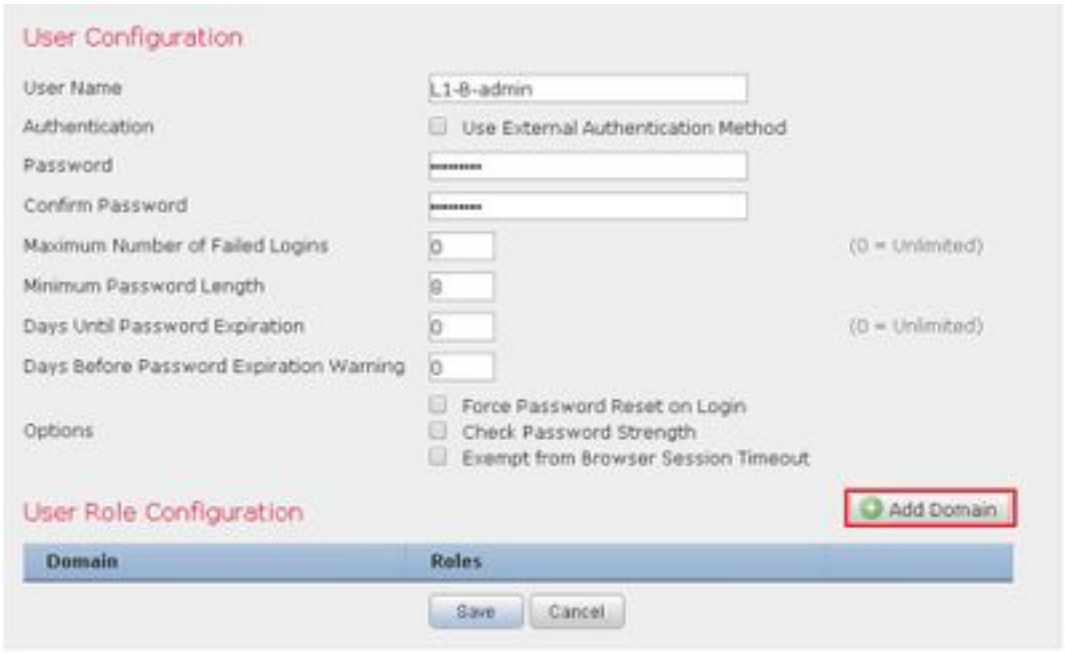
Besturing: **Admin-**gebruikers die tot het betreffende domein behoren, kunnen het beleid BEWERKEN. Om het beleid te bewerken, dat tot andere domeinen (bijvoorbeeld als onderdeel van Inheritance) behoort, moet je het domein van huidige naar een domein overschakelen waarin het Beleid wordt geconfigureerd onder. Alleen gebruikers van Admin die tot het **mondiale** domein of L1-domein behoren, kunnen voor het beleidsbeheer omschakelen rond het onderste domein.

Gebruikers aan domein toevoegen

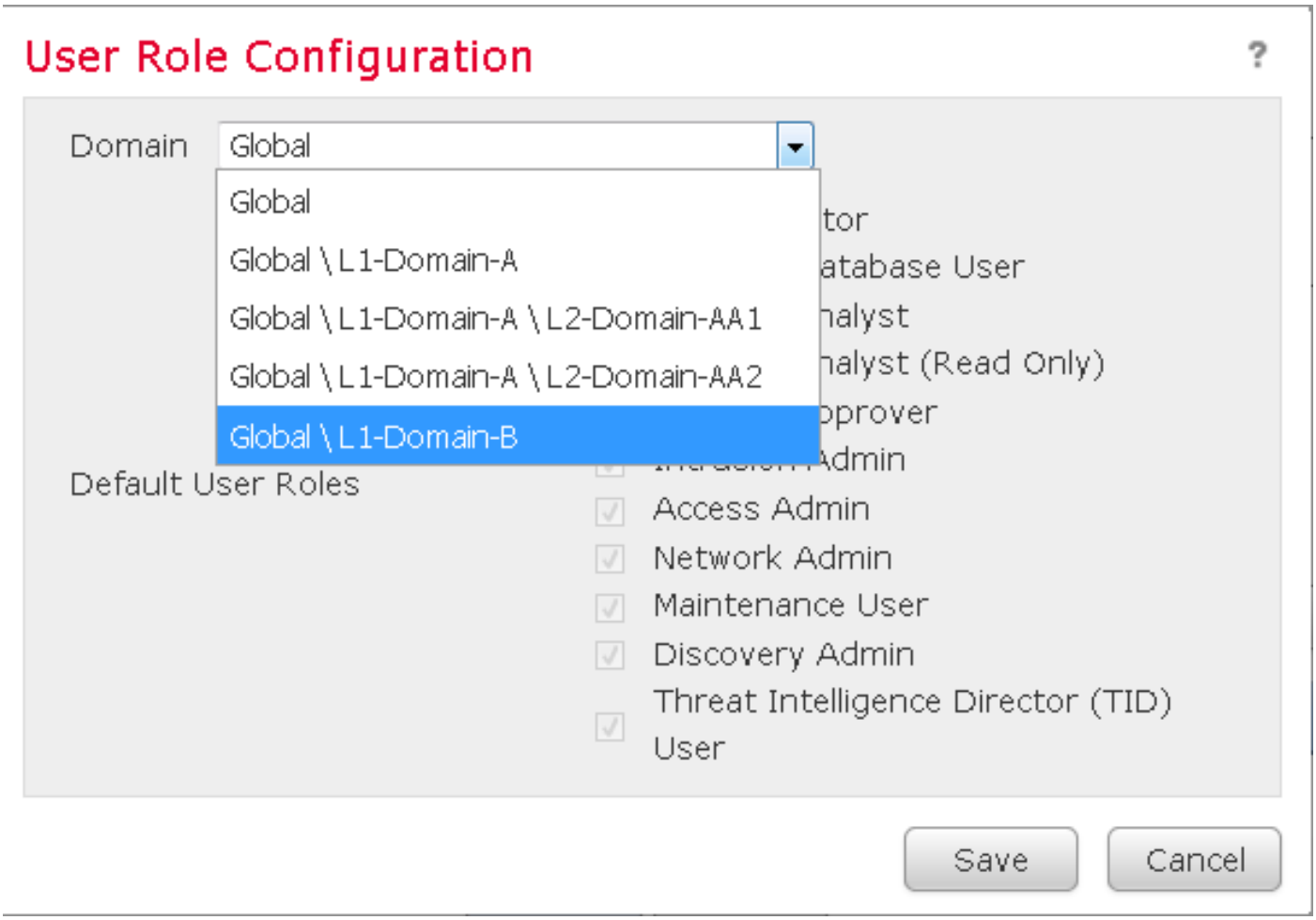
Dit toont hoe u gebruikers in een bepaald domein kunt toevoegen. Deze procedure is van toepassing op gebruikers in de lokale gegevensbank.

1. Blader naar **systeem > gebruikers**. Klik op **Gebruiker maken** zoals in de afbeelding.

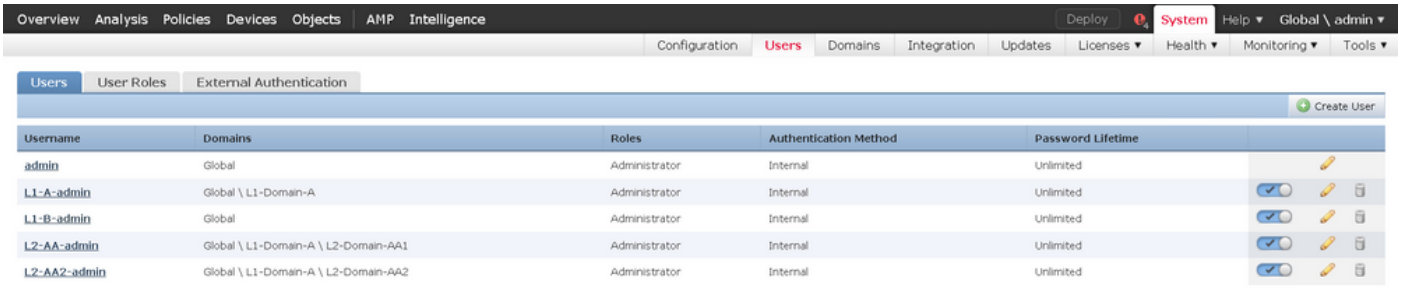
2. Het dialoogvenster **User Configuration** verschijnt. Vul de **gebruikersnaam** en het **wachtwoord in (& Wachtwoord bevestigen)**. Klik op **Add Domain** om de gebruiker aan het gespecificeerde domein toe te voegen zoals in de afbeelding.



3. Selecteer het gewenste domein van de vervolgkeuzelijst Domain waar u de gebruiker onder wilt toevoegen en specificeer de rol zoals die in de afbeelding wordt weergegeven. Een nieuwe gebruiker kan aan het eigen domein of de kinderdomeinen worden toegevoegd.

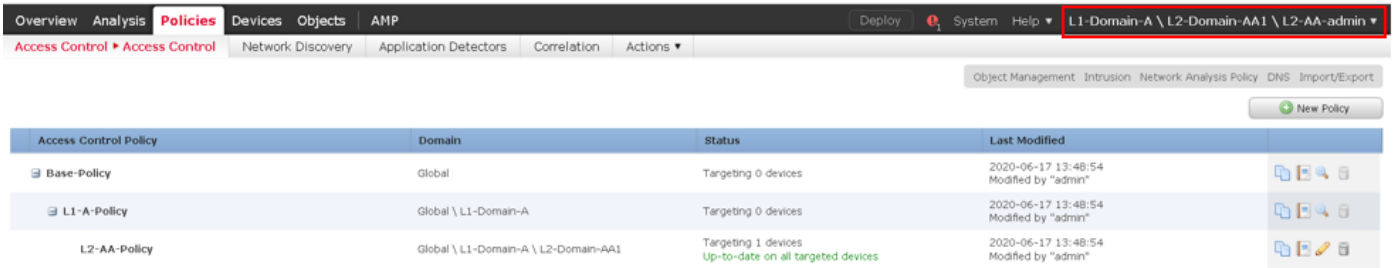


De ingestelde gebruikers worden in deze afbeelding weergegeven:



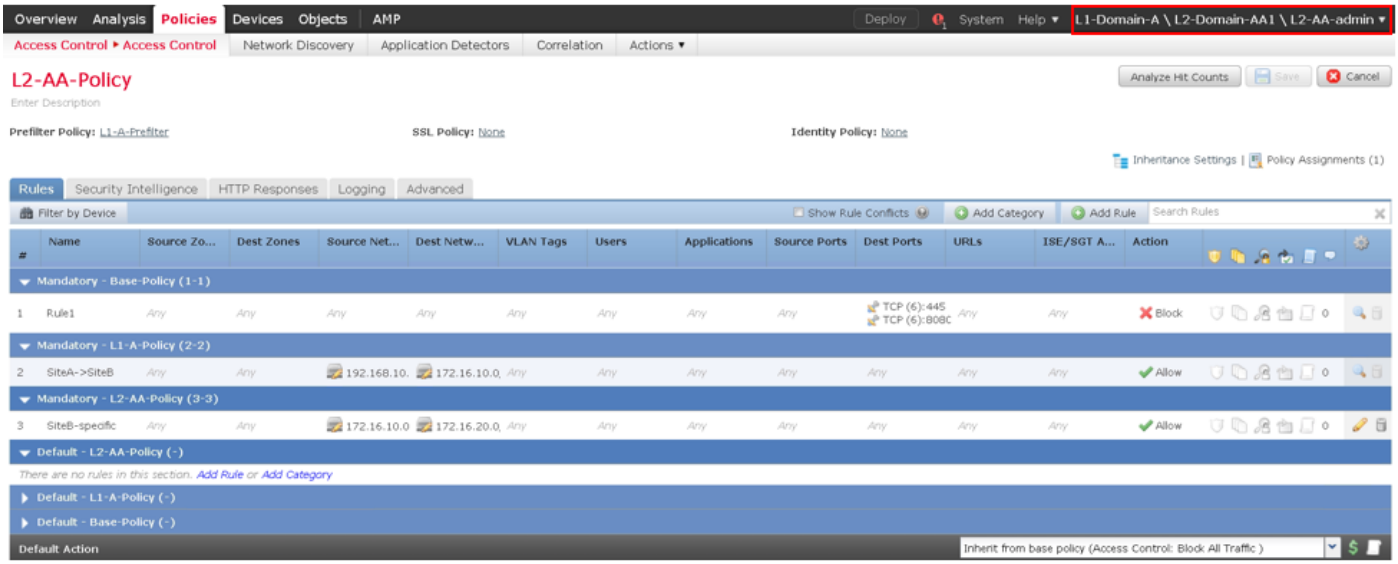
Toegang tot middelen op VMC zou beperkt zijn tot het domein waartoe de gebruiker behoort. Zoals hieronder wordt getoond, wanneer user-**L1-A-admin** zich inlogt bij FMC UI, is de toegang beperkt tot Domain-**L1-Domain-A** waar de gebruiker deel van uitmaakt, en tot het kinderdomein zodra de gebruiker op dat kinderdomein overschakelt. Deze gebruiker kan alleen het beleid bewerken dat in het **L1**-domein-A is gedefinieerd en het beleid dat in het kinderdomein is gedefinieerd wanneer het domein naar het kinderdomein is overgeschakeld. Ook kan uit het onderstaande voorbeeld worden opgemaakt dat **L1-A-Policy** het op het algemene gebied vastgestelde beleid, namelijk **basisbeleid**, erft en kan worden aangepast, wat uit het teken. De overerfingsinstellingen worden uitgevoerd om naar het **basisbeleid te** wijzen zoals in de afbeelding.

Op dezelfde manier heeft een gebruiker **L2-AA-admin** die tot het **L2-Domain-AA1**-domein behoort alleen de controle over het beleid **L2-AA-Policy** dat in het domein wordt gedefinieerd zoals in de afbeelding wordt getoond. Het **L2-AA-Policy** erft het beleid **L1-A-Policy** dat is gedefinieerd in **L1**-Domain-A en dat op zijn beurt **basisbeleid** erft dat in mondiaal domein is gedefinieerd. Daarnaast kan het beleid **L2-AA-Policy** worden aangepast, wat te zien is op de teken. De gebruiker L2-AA-admin kan nooit overschakelen op zijn moederdomein, namelijk L1-Domain-A of zijn voorouderdomein, namelijk het mondiale domein.



Bovendien kan een gebruiker **L1-A-admin** die tot L1-Domain-A behoort, overschakelen op L2-

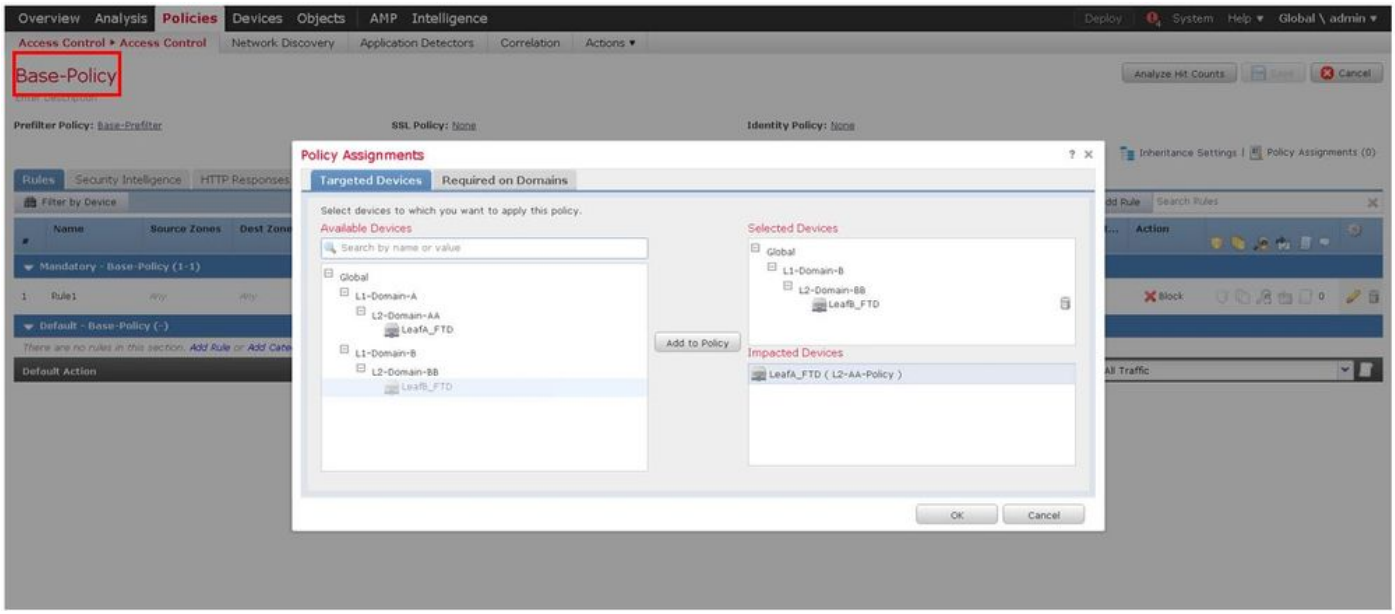
Domain-AA1 en het beleid **L2-AA-Policy** bewerken dat vanaf de teken zoals in de afbeelding. Dit is zelfs van toepassing op een gebruiker die tot het mondiale domein behoort en op de kinderdomeinen overschakelt en het beleid bewerkt dat in het specifieke kinderdomein wordt gedefinieerd.



Belangrijke opmerkingen:

- Wanneer u de niet-mondiale domeinen verwijdert, worden de gebruikers die tot de domeinen behoren automatisch naar het **mondiale** domein verplaatst.

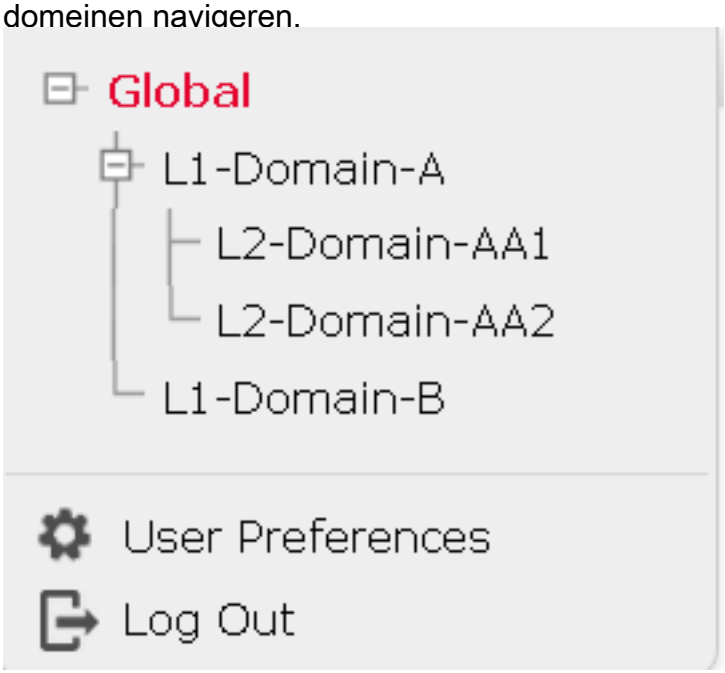
  De FTD/s wordt/worden altijd in het bladdomein gedefinieerd. In dit geval is het bladdomein het **L2-Domain** (d.w.z. L2-Domain-AA en L2-Domain-BB). De FTD die tot **L2-Domein** behoort kan worden toegewezen aan het beleid in **L1-Domain** of in het **Global** Domain. In deze afbeelding hebben de ACS-landen in het mondiale domein de FTD die in het L3-domein is gedefinieerd, toegewezen aan het beleid dat in het mondiale domein is bepaald.



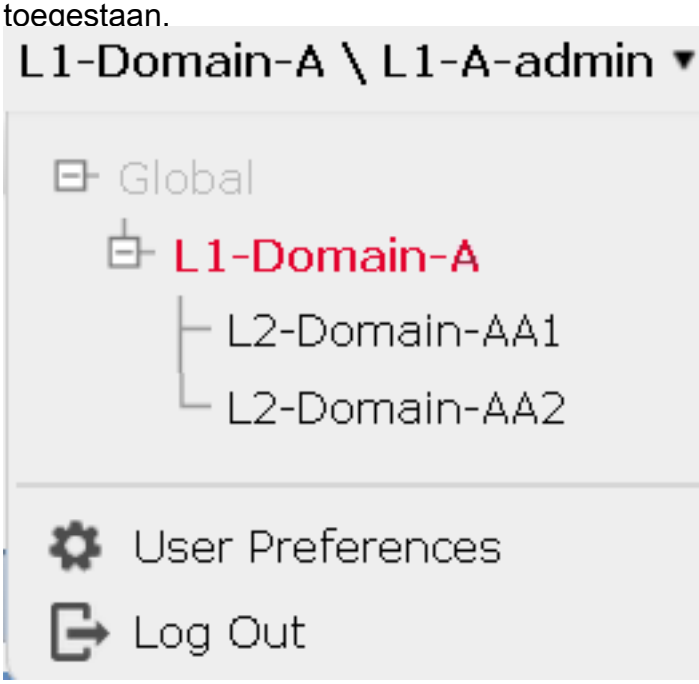
- De gebruikers in het globale domein kunnen naar andere gebruikers-specifieke domeinen navigeren maar de gebruikers van een specifiek domein hebben slechts zichtbaarheid in hun eigen domein en hun kinddomeinen. Ze kunnen niet naar het mondiale domein of naar een ander hoger domein navigeren, zoals in deze tabel wordt getoond:

Wereldwijd domein	Gebruikersspecifiek domein
Gebruiker in het globale domein heeft zichtbaarheid in alle geconfigureerde domeinen en kan naar andere	Gebruiker in **L1-Domain-A** heeft alleen zichtbaarh voor zichzelf en zijn kinderdomein, namelijk **L2-**

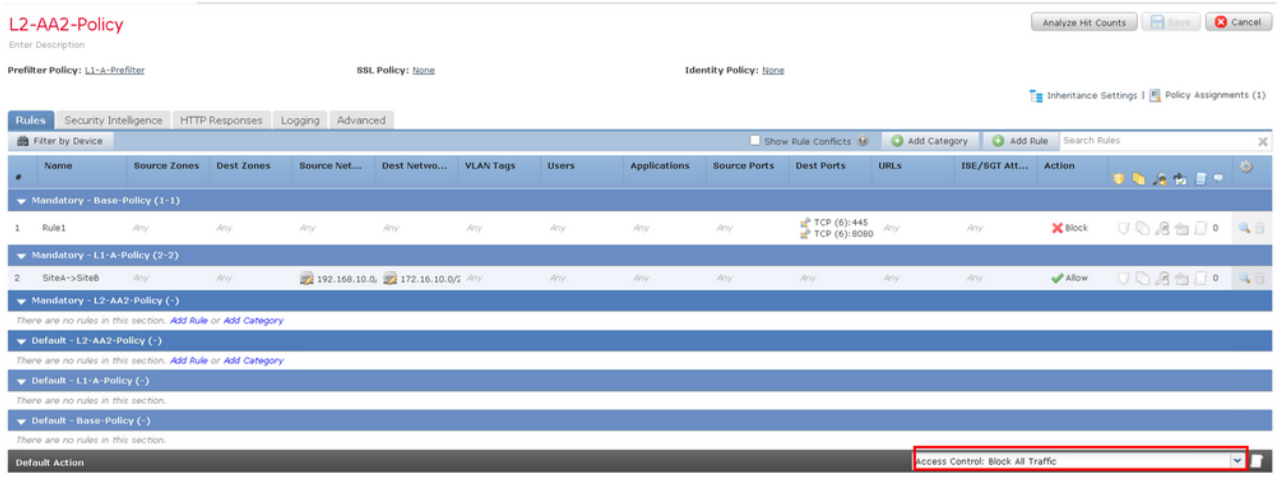
domeinen navigeren.



Domain-AA en kan naar **L2-Domain-AA** navigeren
Toegang op hoger niveau (zoals **Global**) is niet toegestaan.



- De standaardactie van het kinderbeleid kan niet door het ouderbeleid worden vergrendeld en de gebruiker hoeft de standaardactie van het ouderbeleid niet te erven zoals in deze afbeelding.



In deze afbeelding is te zien dat de gebruiker de standaardinstelling niet heeft toegewezen aan de ouder die duidelijk kan worden uit de woorden **Inherit uit het basisbeleid:** niet gezien in een standaardinstelling.

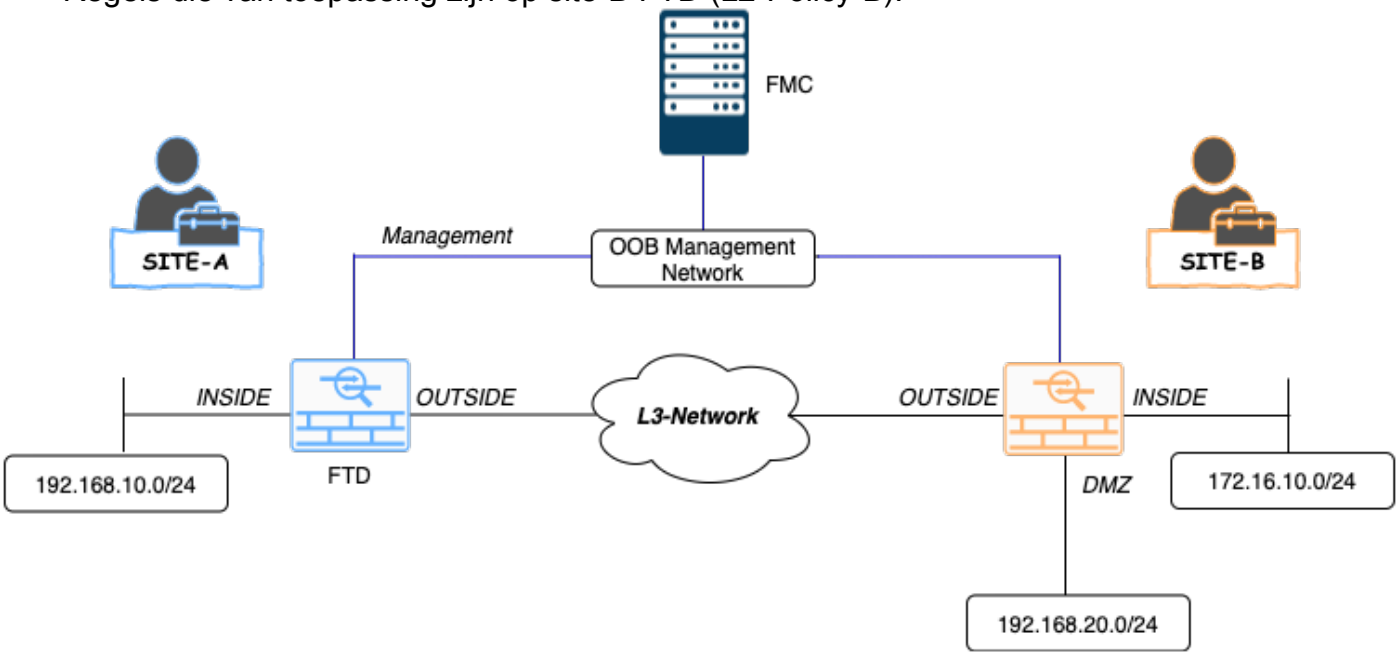
Opmerking: Houd in gedachten dat een gebruiker niet tegelijkertijd zowel het L1- als het L2-domeinbeleid kan weergeven. De gebruiker moet naar het gewenste domein overschakelen om het beleid te bekijken en te bewerken. Bijvoorbeeld: als de gebruiker **admin** die aanwezig is in het globale domein wil bekijken welk beleid in L1-Domain-A en L2-Domain-AA is ingesteld, kan de gebruiker dit doen door over te schakelen op L1-A-Domain om het in dat domein gevormde beleid te bekijken en te bewerken en vervolgens over te schakelen op L2-Domain-AA om het corresponderende beleid te bekijken en te bewerken, maar kan beide niet tegelijkertijd weergeven. Ook kan gebruiker in L1-Domain-A het beleid niet bewerken of verwijderen dat is gedefinieerd in het globale domein, d.w.z. het basisbeleid dat het moederbeleid is van L1-A-Policy, en gebruiker in L2-Domain-AA kan het beleid niet

bewerken of verwijderen, namelijk basisbeleid en L2-A-Policy, gedefinieerd in respectievelijk de globale en L2-Domain-A domeinen.

Case Scenario gebruiken

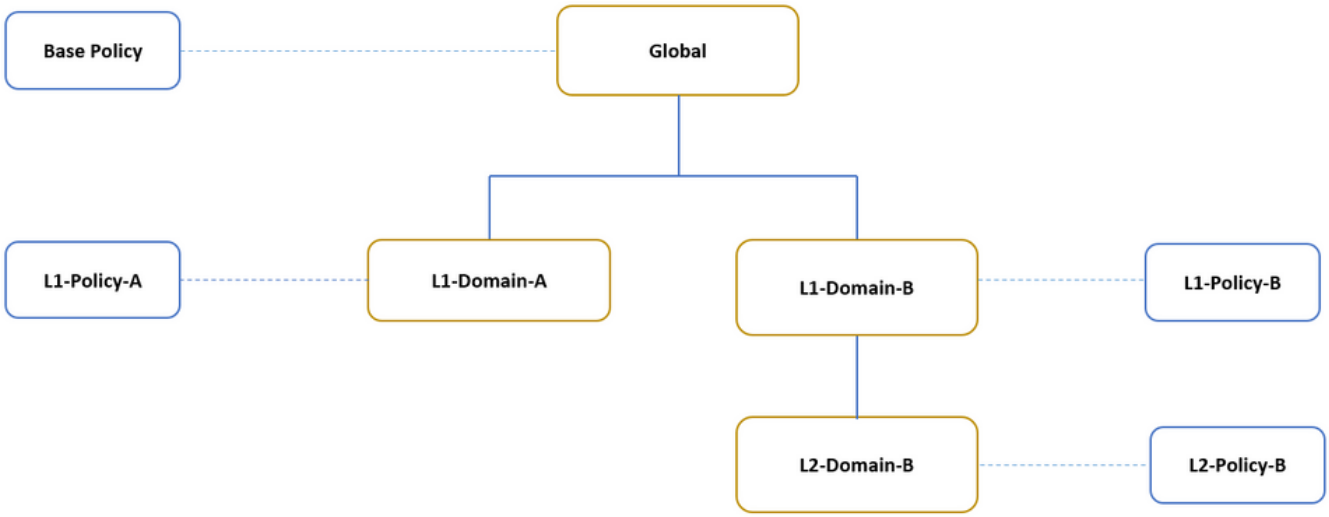
In aanmerking nemend het scenario dat in de afbeelding is afgebeeld, worden FTD's van SITE-A (SiteA-FTD) en SITE-B (SiteB-FTD) door één enkel VCC beheerd via verschillende domeinen (met meerdere domeinen) om gecontroleerde toegang te bieden. Vanuit beleidsoogpunt zijn dit de beleidsoverwegingen op organisatorisch niveau:

- Service-specifieke BLOCK-regels die van toepassing zijn op ALLE FTD's die onafhankelijk zijn van de SITE of DOMAIN, behoren tot (Base-Policy).
- Regels die voldoen aan de vereisten om te voldoen aan site-A tot Site-B toegang (L1-Policy-A) en Site-B tot Site-A toegang (L1-Policy-B).
- Regels die van toepassing zijn op site-B FTD (L2-Policy-B).



Overeenstemming in een omgeving met meerdere domeinen

Voor de hierboven genoemde use case dient u de volgende Domain/Policy hiërarchie te overwegen. SiteA-FTD en SiteB-FTD maken deel uit van de bladdomeinen L1-Domain-A respectievelijk L2-Domain-B.

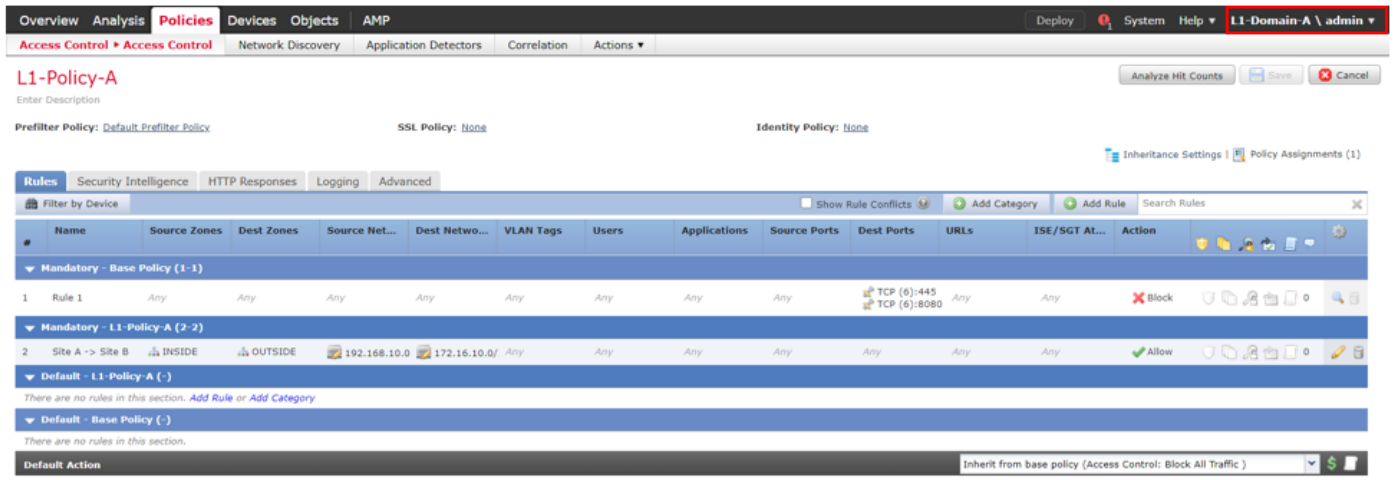


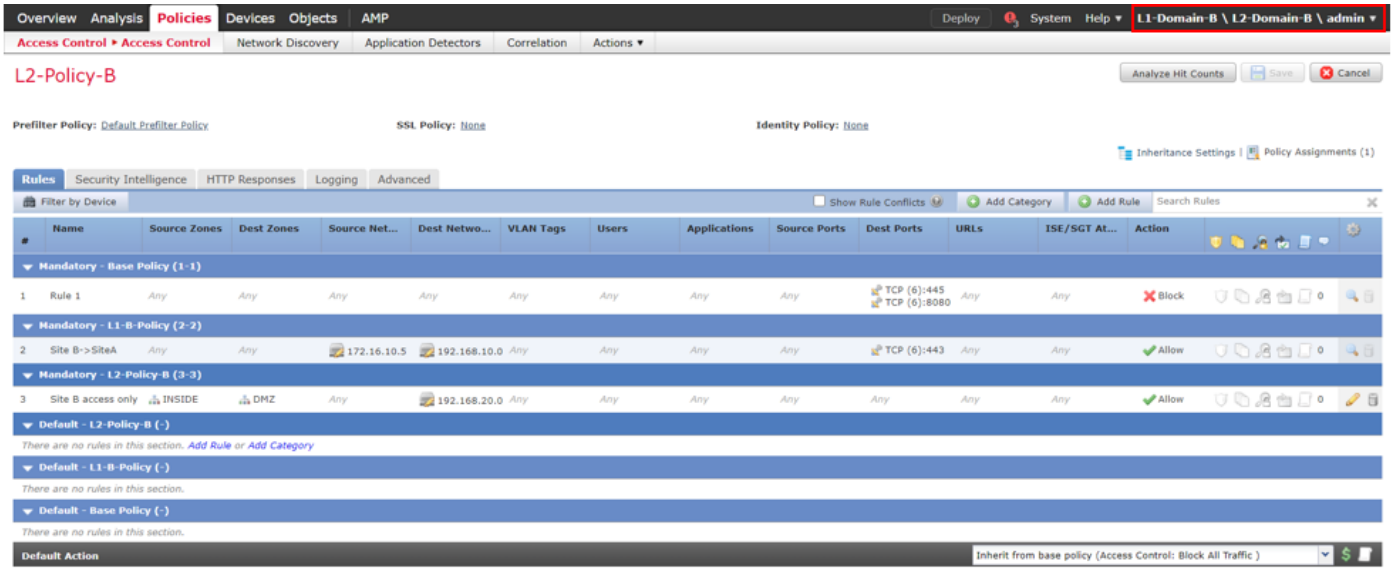
De structuur voor de domeinhiërarchie is als volgt:

- **Global** domain is **parent** of **L1-Domain-A** en **L1-Domain-B**.
- **Mondiaal** domein is **voorouder** van **L2-domein-B**.
- **L2-Domain-B** is kind van **L1-Domain-B**
- **L2-Domain-B** is bladdomein omdat het geen kinddomeinen heeft.

De afbeelding toont de domeinhiërarchie zoals die door FMC wordt gezien.

Hieronder volgt hoe de regels zijn gedefinieerd in **L1-Policy-A** en **L2-Policy-B** w.t naar het bovengenoemde scenario.





U dient altijd de regels en hun erfenis in gedachten te houden bij het configureren van meerdere domeinen om legitieme verkeer te voorkomen of ongewenste verkeer toe te laten.